

REMARKS

Prior to entry of the present amendment, claims 1-18 were pending in the present application. Claims 1 and 10 are amended above. Claims 6, 8, 15 and 17 are cancelled. No new matter is added by the claim amendments. Entry is respectfully requested.

Claims 5 and 14 stand objected to for failure to spell out the abbreviated symbols MD2, MD4, MD5, Snefru, SHA, NIST DSA, Haval, N-Hash and RIPE-MD digital signatures. The claims are amended to spell out the abbreviated symbols. The applicants note that Snefru, Haval and N-Hash are not abbreviated symbols and therefore cannot be spelled out. Reconsideration of the objections to claims 5 and 14 is respectfully requested.

Claims 1-18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Carson (U.S. Patent Number 6,477,124) in view of Gotoh, *et al.* (U.S. Patent Number 6,122,373). Reconsideration of the rejections and allowance of claims 1-18 are respectfully requested.

In the present invention as claimed in independent claim 1, a method of determining the presence of an anomaly region in a digital medium includes performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results, calculating corresponding digital signatures based on data values for each of the multiple read data results, and determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value. If a predetermined number of the digital signatures are not equal in value, the anomaly region is determined to be present.

In the present invention as claimed in independent claim 10, a system for determining whether an anomaly region is present in the digital medium that includes a read unit for performing multiple read operations on a data segment of the medium to generate multiple corresponding read data results, a calculating unit for calculating

corresponding digital signatures for each of the multiple read data results, and a determining unit for determining whether an anomaly region is present in the data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value. If a predetermined number of the digital signatures are not equal in value, the determining unit determines the anomaly region to be present.

Carson discloses, at column 5, lines 7-25, that data on an optical disc can be read from beginning to end or from "lead-in" to "lead-out," or can be accessed in a non-contiguous fashion. Carson further discloses, at column 8, lines 7-43 and at column 9, lines 14-67, a process for disc authentication based on a data rate at which data are written to and read from a disc. In Carson, a data rate profile indicative of the data rate at which data are written to the disc is stored on a disc and used for disc authentication. The data are intentionally written at different, or varying, speeds, at different locations on the disc, and a measured data rate as a function of position on the disc is used to create the data rate profile. Variance in the data rate at which data are written to the disc results in the pits and lands written to the disc having different sizes, depending on the velocity of the disk at the time and position at which the given pits and lands are written. Authentic discs will include data that are recorded in accordance with the data rate profile and non-authentic discs will not. During playback, a readback system will attempt to speed up and slow down the rotation of the disc to maintain a substantially constant recovered data rate. The behavior of the readback system during readback is monitored, recorded, and analyzed to form a data rate profile for the disc in question. When an unauthorized duplicate disc is created, the expected data rate profile will not be present on the unauthorized duplicate disc because an unauthorized disc will not have variance in the lengths of its pits and lands at expected locations on the disc. During a subsequent reading operation of a disc, the actual velocity of the disc at certain locations can be compared to the expected velocity at those locations to authenticate the disc. If a mismatch occurs, the disc is determined to be an unauthorized disc and access to the disc can be prevented. If no mismatch is detected, full disc access can be granted.

Carson fails to teach or suggest a method of determining the presence of an anomaly region in a digital medium that includes “calculating corresponding digital signatures based on data values for each of...multiple read data results,” and “determining whether an anomaly region is present in” a “data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determines the anomaly region to be present,” as claimed in independent claim 1. Carson further fails to teach or suggest a system for determining the presence of an anomaly region in a digital medium that includes “a calculating unit for calculating corresponding digital signatures based on data values for each of...multiple read data results,” and “a determining unit for determining whether an anomaly region is present in” a “data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determining the anomaly region to be present,” as claimed in independent claim 10.

As stated above, in the invention as claimed in claims 1 and 10, the “digital signatures” are calculated “based on data values for each of the multiple read data results.” That is, the data values of the underlying data that are read during the multiple read operations is used to calculate the digital signatures. Carson does not teach or suggest this feature. Instead, in Carson, the authentication process is based on the rate at which data are written to and read from the disc. In Carson, there is no significance to the underlying data values in authenticating the disc.

Further, in the invention as claimed in claims 1 and 10, an anomaly region is determined to be present on the disc in the event that a predetermined number of the digital signatures resulting from the underlying data read during the multiple read operations are “not equal in value,” or different. In contrast, Carson teaches the inverse; namely that an anomaly region (different sized pits and lands) is determined to be present on the disc in the event that the data rate profiles (measured and expected) are determined to be equal in value, or the same.

Gotoh, *et al.* discloses that at a press factory 4501, an ID number and its corresponding digital signature are recorded as a barcode in a PCA area of an optical disk 4506 using a PCA writer 4507. A public key is prerecorded on a master disk that is in a pit portion of the disk. When the optical disk 4506 is loaded into a playback apparatus, the public key is read from the pit portion and the ID number and the digital signature appended to it are read from the PCA area and decrypted with the public key. A verification section 4511 determines whether the digital signature is legitimate or illegitimate. If the digital signature data is found to be illegitimate as a result of the verification, the playback operation of the optical disk is stopped. If the digital signature data is found to be legitimate as a result of the verification, the playback operation of the optical disk is allowed to continue.

Like Carson, Gotoh, *et al.* fails to teach or suggest a method of determining the presence of an anomaly region in a digital medium that “calculating corresponding digital signatures based on data values for each of...multiple read data results,” and “determining whether an anomaly region is present in” a “data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determines the anomaly region to be present,” as claimed in independent claim 1. Gotoh, *et al.* further fails to teach or suggest a system for determining the presence of an anomaly region in a digital medium that includes “a calculating unit for calculating corresponding digital signatures based on data values for each of...multiple read data results,” and “a determining unit for determining whether an anomaly region is present in” a “data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, and if a predetermined number of the digital signatures are not equal in value, the determining unit determining the anomaly region to be present,” as claimed in independent claim 10. There is no teaching or suggestion in Gotoh, *et al.* that the digital signatures are calculated “based on data values” for each of the multiple read results. In addition, in Gotoh, *et al.*, there is no teaching or suggestion that digital signatures of multiple read operations are compared to each other or that the comparison is used to determine whether an anomaly is present on the disc.

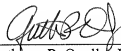
Carson and Gotoh, *et al.* fail to teach or suggest a method of determining the presence of an anomaly region in a digital medium that includes “calculating corresponding digital signatures based on data values for each of...multiple read data results,” and “determining whether an anomaly region is present in” a “data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, if a predetermined number of the digital signatures are not equal in value, the determining unit determines the anomaly region to be present,” as claimed in independent claim 1, and a system for determining the presence of an anomaly region in a digital medium that includes “a calculating unit for calculating corresponding digital signatures based on data values for each of...multiple read data results,” and “a determining unit for determining whether an anomaly region is present in” a “data segment based on a comparison of the digital signatures by determining whether any of the digital signatures are equal in value, if a predetermined number of the digital signatures are not equal in value, the determining unit determining the anomaly region to be present,” as claimed in independent claim 10. Since neither of Carson and Gotoh, *et al.* teach or suggest the limitations of independent claims 1 and 10, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claims 1 and 10 under 35 U.S.C. 103(a) as being unpatentable over Carson and Gotoh, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 2-9 and 11-18, it follows that this claim should inherit the allowability of the independent claims from which they depend.

Closing Remarks

It is submitted that all claims are in condition for allowance, and such allowance is respectfully requested. If prosecution of the application can be expedited by a telephone conference, the Examiner is invited to call the undersigned at the number given below.

Respectfully submitted,

Date: February 15, 2008
Mills & Onello, LLP
Eleven Beacon Street, Suite 605
Boston, MA 02108
Telephone: (617) 994-4900, Ext. 4902
Facsimile: (617) 742-7774
J:\ECD\0014CIP\amendmenta2.doc



Anthony P. Onello, Jr.
Registration Number 38,572
Attorney for Applicant